Mark

What is SSH key?

Mark Jul 5, 2018 · 2 min read

SSH key is a credential in SSH protocol. The function is similar to your username and password. SSH key is a key pair, included a privacy key and a public key.

Public key can be shared to others and can be easily generated from privacy key. Privacy key **MUST NOT** be shared to others and cannot be easily generated from public key (based on current computational power).

User Keys & Host Keys

SSH key implementation supports host to access remote server and remote server access host (you can think as your personal computer).

When user accesses remote server, it is called **User Keys**.

When remote server access host (e.g. your PC), it is called **Host Keys**.

How User Keys work?

We use an example to explain how you use your computer to access a remote server.

1. client generates public key and privacy key [`ssh-keygen`]
2. client copies public key to remote server [`ssh-copy-id`]
3. server stores the public key
4. when client wants to connect to remote server, it initiates a connection to server via SSH protocol [`ssh <username>@<ipAddress>`]

5. remote server receives the connection from client
6. remote server identifies which public key should be used based on protocol
7. remote server uses public key to encrypt a random message
8. remote server sends the encrypted message to client
9. client uses private key to decrypt the message
10. client sends the decrypted message and previous session ID to remote server
11. remote server verifies the decrypted message from client,

which is matched the sent message or not

12. if match, client gains access to remote server

How Host Keys work?

The implementation is similar to user keys. The public key and privacy key is stored in remote server and the public key is stored in host.

Why I need to use SSH key?

It can protect your data via the Internet, e.g. prevent man-in-the-middle.

Encryption and Size of SSH key

There are different size of the SSH keys, one of the suggested encryption is `RSA 2048-bit encryption`. The key is a 617-digit number.

Where can I find my key?

In your computer, it usually store in `.ssh/`. In remote server, it suggests to use a management key tools to manage the key due to the number of key. It can be a large number if your services is used by many parties.

Ssh | Explanation | Ssh Keys | User Keys | Host Keys